THAT WHICH IS CLAIMED:

1. A dynamically reconfigurable intrusion-tolerant network interposed between a service requesting client and a protected server to minimize the impact of intrusive events comprising:

a proxy server for receiving network service requests from a client and forwarding said requests pursuant to a tolerance protocol to a protected server, and responding to a client;

an acceptance monitor for receiving from the protected server one or more responses to the client request and applying one or more acceptance tests thereto; and

a ballot monitor for receiving from the acceptance monitor the results of the applied acceptance tests and determining a preferred response to the client request

2. A dynamically reconfigurable intrusion-tolerant network interposed between a service requesting client and a protected server to minimize the impact of intrusive events comprising:

a proxy server for receiving network service requests from a client and forwarding said requests pursuant to a tolerance protocol to a protected server, and responding to a client;

an acceptance monitor for receiving from the protected server one or more responses to the client request and applying one or more acceptance tests thereto;

a ballot monitor for receiving from the acceptance monitor the results of the applied acceptance tests and determining a preferred response to the client request;

an intrusion sensor responsive to anomalies in operation of the network for detecting threats to the network; and

an adaptive reconfigurer for altering the tolerance protocol and reconfiguring a network forwarding scheme among the proxy server, acceptance monitor and ballot monitor in response to a predetermined condition.

3. A network according to Claim 1 wherein said proxy server further forwards said requests to an acceptance monitor and a ballot monitor.

4. A network according to Claim 1 wherein said proxy server comprises multiple independent proxy servers.

5. A network according to Claim 1 wherein said acceptance monitor comprises multiple independent acceptance monitors.

6. A network according to Claim 1 wherein said ballot monitor comprises multiple independent ballot monitors.

7. A network according to Claim 2 wherein said intrusion sensor comprises a multiplicity of sensors monitoring predetermined operations of the network.

8. A network according to Claim 2 wherein said adaptive reconfigurer reconfigures the network forwarding scheme to establish parallel forwarding among the protected server, acceptance monitor, and ballot monitor.

9. A network according to Claim 1 wherein said proxy server forwards said requests to a protective server, the acceptance monitor and the ballot monitor.

10. A network according to Claim 1 wherein said acceptance monitor applies one or more acceptance tests taken from the group of satisfaction of requirements test, accounting test, reasonableness test or computer run time test.

11. A network according to Claim 1 wherein said ballot monitor determines a preferred response using a process taken from the group of: simple majority voting, Byzantine agreement process, or adjudication process.

12. A network according to Claim 1 wherein said proxy server forwards said requests to multiple independent protected servers.

13. A network according to Claim 12 wherein said acceptance monitor receives responses from multiple protective servers and applies independent acceptance tests to each received response.

14. A network according to Claim 13 wherein said ballot monitor receives responses from multiple acceptance monitors and determines a preferred response from the multiple responses received.

15. A network according to Claim 2 wherein at least one of said proxy server, acceptance monitor, ballot monitor, intrusion sensor and adaptive reconfigurer comprise a separate and independent processor.

16. A network according to Claim 2 wherein two or more of said proxy server, acceptance monitor, ballot monitor, intrusion sensor and adaptive reconfigurer operate on a single processor.

17. A network according to Claim 2 wherein the adaptive reconfigurer reconfigures the network forwarding scheme to establish multiple independent network forwarding paths.

18. A method for reconfiguring communication among network components to minimize the impact of intrusive events, comprising:

receiving a network service request and forwarding the request pursuant to a tolerance protocol;

generating a response to the service request and forwarding the response;

applying one or more acceptance tests to the response and forwarding the test results;

polling the test results to determine a preferred response based upon the poll; and

forwarding the preferred response to the client.

19. A method for dynamically reconfiguring communication among network components pursuant to multiple tolerance protocols to minimize the impact of intrusive events, comprising:

receiving a network service request and forwarding the request pursuant to a tolerance protocol;

generating a response to the service request and forwarding the response;

applying one or more acceptance tests to the response and forwarding the test results;

polling the acceptance test results to determine a preferred response based upon the poll;

forwarding the preferred response to the client;

detecting any anomalies in operation of the network; and

revising the tolerance protocol and a network forwarding scheme in response to an anomaly in operation of the network.

20. A method according to Claim 18 wherein the step of receiving a network service request further comprises receiving a network service request at a proxy server.

21. A method according to Claim 18 wherein the step of receiving a network service request further comprises forwarding a request to at least one protected server.

22. A method according to Claim 18 wherein the step of receiving a network service request further comprises forwarding the request to multiple protected servers.

23. A method according to Claim 18 wherein the step of receiving a network service request further comprises forwarding the request on multiple independent paths.

24. A method according to Claim 18 wherein the step of generating a response comprises generating a response at a protected server.

25. A method according to Claim 18 wherein the step of generating a response and forwarding the response comprises forwarding a response to an acceptance monitor.

26. A method according to Claim 18 wherein the step of generating a response and forwarding a response comprises forwarding the response to multiple acceptance monitors.

27. A method according to Claim 18 wherein the step of generating a response and forwarding a response comprises forwarding the response on multiple independent paths.

28. A method according to Claim 18 wherein the step of applying one or more acceptance tests comprises applying one or more acceptance tests at an acceptance monitor.

29. A method according to Claim 18 wherein the step of applying one or more acceptance tests comprises applying independent acceptance tests to each response.

30. A method according to Claim 18 wherein the step of applying one or more acceptance tests and forwarding the test results comprises forwarding the test results to a ballot monitor.

31. A method according to Claim 18 wherein the step of applying one or more acceptance tests and forwarding the test results comprises forwarding the tests results to multiple ballot monitors.

32. A method according to Claim 18 wherein the step of applying one or more acceptance tests and forwarding the test results comprises forwarding the tests results on multiple independent paths.

33. A method according to Claim 18 wherein the step of polling the acceptance test results comprises polling the acceptance test results at a ballot monitor.

34. A method according to Claim 18 wherein the step of polling the acceptance test results comprises applying multiple polling routines.

35. A method according to Claim 18 wherein the step of polling the acceptance test results comprises applying multiple polling routines to the responses from each of a multiplicity of ballot monitors.

36. A method according to Claim 18 wherein at least one of the steps of receiving a network service request, generating a response to a service request, applying one or more acceptance tests, polling the acceptance test results and forwarding the preferred response to a client comprises utilizing a separate processor to enhance independence of operation and minimize the impact of intrusive events.

37. A method according to Claim 19 wherein the step of revising the tolerance protocol and network forwarding scheme comprises forwarding on multiple independent paths.

38. A method according to Claim 19 wherein the step of revising the tolerance protocol and network forwarding scheme comprises forwarding to multiple independent acceptance monitors.

39. A method according to Claim 19 wherein the step of revising the tolerance protocol and network forwarding scheme comprises forwarding to multiple independent ballot monitors.

40. A method according to Claim 19 wherein the step of revising the tolerance protocol and network forwarding scheme comprises forwarding to multiple independent proxy servers.

41. A method according to Claim 19 wherein the step of revising the tolerance protocol and network forwarding scheme further comprises comparing any detected anomalies with known anomalies to identify a predetermined intrusion tolerance protocol.

42. A method according to Claim 19 wherein the step of revising the tolerance protocol and network forwarding scheme comprises determining the acceptance monitors that will be used to support the selected tolerance protocol.

43. A method according to Claim 19 wherein the step of revising the tolerance protocol and network forwarding scheme comprises determining the ballot monitors that will be used to support the selected tolerance protocol.

44. A method according to Claim 19 wherein the step of revising the tolerance protocol and network forwarding scheme comprises determining the proxy servers that will be used to implement the selected tolerance protocol.

45. A method according to Claim 19 wherein the step of revising the tolerance protocol and network forwarding scheme comprises prioritizing the network service requests.